



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/788,670	02/21/2001	Hartvig W.J. Ekner	12135-006001/0113.00US	6040

26171 7590 04/22/2004

FISH & RICHARDSON P.C.  
1425 K STREET, N.W.  
11TH FLOOR  
WASHINGTON, DC 20005-3500

EXAMINER

DO, CHAT C

ART UNIT PAPER NUMBER

2124

DATE MAILED: 04/22/2004

9

Please find below and/or attached an Office communication concerning this application or proceeding.

Handwritten signature

# Office Action Summary

Application No.

09/788,670

Applicant(s)

EKNER ET AL.

Examiner

Chat C. Do

Art Unit

2124

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 13 February 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-42 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. This communication is responsive to Amendment A, filed 2/13/2004.
2. Claims 1-42 are pending in this application. Claims 1, 15, and 29 are independent claims. In Amendment A, claims 1, 14-15, 28-29, and 42 are amended. This action is made final.

#### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6, 9-20, 23-34, and 37-42 are rejected under 35 U.S.C. 102(e) as being anticipated by Bhandal et al. (U.S. 6,711,602).

Re claim 1, Bhandal et al. disclose in Figures 5 and 7-8 a multiply unit (abstract) comprising: at least one input data path (all the paths connect the src1&2 to multipliers in Figure 5) for receiving one or more input operands (SRC1 and SRC2) to the multiply unit (Figure 5); an arithmetic multiplier (171) connected to receive the one or more input operands (SRC1 and SRC2); a binary polynomial multiplier (164) connected to receive the one or more input operands (SRC1 and SRC2) and including components separate and distinct from

components of the arithmetic multiplier (164 is distinct from 171); and a multiply unit output data path (Figure 8) connected to receive an output of the arithmetic multiplier (output of 830) and connected to receive an output of the binary polynomial multiplier (output of 860).

Re claim 2, Bhandal et al. further disclose in Figure 7 the arithmetic multiplier includes a multiplier array (all levels of CSA in Figure 7).

Re claim 3-5, Bhandal et al. further disclose in Figure 7 the multiplier array is a Wallace tree multiplier array (all levels of CSA arrangement) including a plurality of carry-save adders (CSA) in a tree structure and carry-propagate adder.

Re claim 6, Bhandal et al. further disclose in Figures 5 and 7-8 comprising Booth recoding logic (710b).

Re claim 9, Bhandal et al. further disclose in Figures 5 and 7-8 the binary polynomial multiplier includes a binary polynomial multiplication array (col. 6 lines 27-34).

Re claim 10, Bhandal et al. further disclose in Figures 5 and 7-8 the binary polynomial multiplier (abstract) includes a polynomial multiplication array having a first input (SRC1) and a second input (SRC2), the polynomial multiplication array including: a plurality of row multipliers (Figures 14-15) that multiply the first input by a bit of the second input; and at least one adder (CSA adders) for computing a result by adding the results from the plurality of row multipliers.

Re claim 11, Bhandal et al. further disclose in Figures 5 and 7-8 the at least one adder performs a bitwise exclusive-or on the results from the plurality of row multipliers (XOR in Figure 14).

Re claim 12, Bhandal et al. further disclose in Figures 5 and 7-8 at least one of the plurality of row multipliers performs multiplication by computing a logical AND of the first input and a bit of the second input (AND in Figure 14).

Re claim 13, Bhandal et al. further disclose in Figures 5 and 7-8 comprising an accumulator, and wherein the at least one adder computes a result by adding the results from the plurality of row multipliers and the accumulator (117).

Re claim 14, Bhandal et al. further disclose a permutation logic connected to receive the one or more input operands and operable to produce an output comprising a permutation of the one or more input operands (all the logic components that routes the SRC1 and SRC2 to the multipliers in Figure 5 and col. 8 lines 11-14).

Re claim 15, it is a processor claim of claim 1. Thus, claim 15 is also rejected under the same rationale in the rejection of rejected claim 1.

Re claim 16, it is a processor claim of claim 2. Thus, claim 16 is also rejected under the same rationale in the rejection of rejected claim 2.

Re claim 17, it is a processor claim of claim 3. Thus, claim 17 is also rejected under the same rationale in the rejection of rejected claim 3.

Re claim 18, it is a processor claim of claim 4. Thus, claim 18 is also rejected under the same rationale in the rejection of rejected claim 4.

Re claim 19, it is a processor claim of claim 5. Thus, claim 19 is also rejected under the same rationale in the rejection of rejected claim 5.

Re claim 20, it is a processor claim of claim 6. Thus, claim 20 is also rejected under the same rationale in the rejection of rejected claim 6.

Re claim 23, it is a processor claim of claim 9. Thus, claim 23 is also rejected under the same rationale in the rejection of rejected claim 9.

Re claim 24, it is a processor claim of claim 10. Thus, claim 24 is also rejected under the same rationale in the rejection of rejected claim 10.

Re claim 25, it is a processor claim of claim 11. Thus, claim 25 is also rejected under the same rationale in the rejection of rejected claim 11.

Re claim 26, it is a processor claim of claim 12. Thus, claim 26 is also rejected under the same rationale in the rejection of rejected claim 12.

Re claim 27, it is a processor claim of claim 13. Thus, claim 27 is also rejected under the same rationale in the rejection of rejected claim 13.

Re claim 28, it is a processor claim of claim 14. Thus, claim 28 is also rejected under the same rationale in the rejection of rejected claim 14.

Re claim 29, it is a computer-readable medium claim of claim 1. Thus, claim 29 is also rejected under the same rationale in the rejection of rejected claim 1.

Re claim 30, it is a computer-readable medium claim of claim 2. Thus, claim 30 is also rejected under the same rationale in the rejection of rejected claim 2.

Re claim 31, it is a computer-readable medium claim of claim 3. Thus, claim 31 is also rejected under the same rationale in the rejection of rejected claim 3.

Re claim 32, it is a computer-readable medium claim of claim 4. Thus, claim 32 is also rejected under the same rationale in the rejection of rejected claim 4.

Re claim 33, it is a computer-readable medium claim of claim 5. Thus, claim 33 is also rejected under the same rationale in the rejection of rejected claim 5.

Re claim 34, it is a computer-readable medium claim of claim 6. Thus, claim 34 is also rejected under the same rationale in the rejection of rejected claim 6.

Re claim 37, it is a computer-readable medium claim of claim 9. Thus, claim 37 is also rejected under the same rationale in the rejection of rejected claim 9.

Re claim 38, it is a computer-readable medium claim of claim 10. Thus, claim 38 is also rejected under the same rationale in the rejection of rejected claim 10.

Re claim 39, it is a computer-readable medium claim of claim 11. Thus, claim 39 is also rejected under the same rationale in the rejection of rejected claim 11.

Re claim 40, it is a computer-readable medium claim of claim 12. Thus, claim 40 is also rejected under the same rationale in the rejection of rejected claim 12.

Re claim 41, it is a computer-readable medium claim of claim 13. Thus, claim 41 is also rejected under the same rationale in the rejection of rejected claim 13.

Re claim 42, it is a computer-readable medium claim of claim 14. Thus, claim 42 is also rejected under the same rationale in the rejection of rejected claim 14.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 7-8, 21-22, and 35-36 are rejected under 35 U.S.C. 103(a) as being obvious over Bhandal et al. (U.S. 6,711,602) in view of Magar (U.S. 4,538,239).

Re claims 7, Bhandal et al. do not disclose in Figures 5 and 7-8 the arithmetic multiplier performs 32-bit by 16 bit multiplications in a two clock cycles. However, Magar disclose in Figure 3 that an arithmetic multiplier performs 16x16 multiplications in a two clock cycles back in 1985. As the technology improve, more multiplications can be processed in less cycles.

Therefore, it would have been obvious to a person having ordinary skill in the art



at the time the invention is made to perform 32x16 multiplications in a two clock cycles as seen in Magar's invention into Bhandal et al.'s invention because it would enable to improve the system performance.

Re claim 8, Bhandal et al. do not disclose in Figures 5 and 7-8 the arithmetic multiplier performs 32-bit by 32 bit multiplications in three clock cycles. However, Magar disclose in 3 that an arithmetic multiplier performs 16x16 multiplications in a two clock cycles back in 1985. As the technology improve, more multiplications can be processed in less cycles. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to perform 32x32 multiplications in a three clock cycles into Bhandal et al.'s invention because it would enable to improve the system performance.

Re claim 21, it is a processor claim of claim 7. Thus, claim 21 is also rejected under the same rationale in the rejection of rejected claim 7.

Re claim 22, it is a processor claim of claim 8. Thus, claim 22 is also rejected under the same rationale in the rejection of rejected claim 8.

Re claim 35, it is a computer-readable medium claim of claim 7. Thus, claim 35 is also rejected under the same rationale in the rejection of rejected claim 7.

Re claim 36, it is a computer-readable medium claim of claim 8. Thus, claim 36 is also rejected under the same rationale in the rejection of rejected claim 8.

Art Unit: 2124

7. Claims 14, 28, and 42 are rejected under 35 U.S.C. 103(a) as being obvious over Bhandal et al. (U.S. 6,711,602) in view of Zhijie et al. ("Bit Permutation Instructions for Accelerating Software Cryptography").

Re claim 14, Bhandal et al. do not disclose a permutation logic connected to receive the one or more input operands and operable to produce an output comprising a permutation of the one or more input operands. However, Zhijie et al. disclose that a permutation logic is widely known and used in cryptographic algorithms (abstract). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a permutation logic receive the one or more input operands and operable to produce an output of one or more input operands into Bhandal et al.'s invention because it would enable to implement the cryptography algorithm efficiently and more secure (2<sup>nd</sup> page 3<sup>rd</sup> paragraph).

Re claim 28, it is a processor claim of claim 14. Thus, claim 28 is also rejected under the same rationale in the rejection of rejected claim 14.

Re claim 42, it is a computer-readable medium claim of claim 14. Thus, claim 42 is also rejected under the same rationale in the rejection of rejected claim 14.

### ***Response to Arguments***

8. Applicant's arguments with respect to claims 1-42 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
- a. U.S. Patent No. 6,073,154 to Dick discloses a computing multidimensional DFTS in FPGA.
  - b. U.S. Patent No. 4,852,037 to Aoki discloses an arithmetic unit for carrying out both multiplication and addition in an interval for the multiplication.
  - c. U.S. Patent No. 5,396,502 to Owsley et al. disclose a single-stack implementation of a reed-solomon encoder/decoder.
10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).
- A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Art Unit: 2124

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (703) 305-5655.

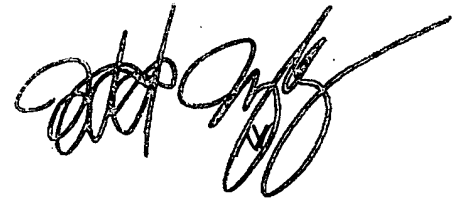
The examiner can normally be reached on M => F from 7:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chaki Kakali can be reached on (703) 305-9662. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chat C. Do  
Examiner  
Art Unit 2124

April 12, 2004

A handwritten signature in black ink, appearing to read 'TODD INGBERG', with a long, sweeping horizontal line extending to the right.

**TODD INGBERG  
PRIMARY EXAMINER**